

WHAT IS CLAIMED IS:

1. デジタルデータを配信する配信サーバーと、
前記配信サーバーから配信されるデジタルデータを受信する受信端末と、
前記受信端末が受信したデジタルデータの書き込み先となる記録媒体と、
前記受信端末が受信したデジタルデータを前記記録媒体へ書き込むアダプタと
によって構成されるデジタルデータ配信システムであって、
前記受信端末は、
前記配信サーバーにアクセスするための通信手段と、
前記配信サーバーから送られてくる情報を閲覧しそれに応答するためのブラウズ手段
と、
前記アダプタとの接続を制御するアダプタ接続制御手段と
を有することを特徴とし、
前記記録媒体は、
改竄不可能な、その記録媒体を一意に識別することのできる固有の情報である媒体 I
Dを有することを特徴とし、
前記アダプタは、
セキュア通信手段と、
そのアダプタを一意に識別することのできるアダプタ I Dと、
前記アダプタ I Dを抽出し、前記配信サーバーへ送信するアダプタ I D検出手段と、
前記記録媒体から、前記媒体 I Dを抽出し、前記配信サーバーへ送信する媒体 I D検
出手段と、
前記記録媒体にたいしてデータの読み書きを行う記録媒体アクセス手段と、
前記記録媒体アクセス手段による前記記録媒体への読み書きを制御する媒体アクセス
処理制御手段と
を有することを特徴とし、
前記配信サーバーは、
セキュア通信手段と、

情報やデジタルデータを前記受信端末に送受信するための送受信手段と、
ユーザーへ送信する情報の生成およびユーザーからのアクセスを処理する配信フロントエンドと、
ユーザーIDと関連するユーザーのアカウント情報を記録するユーザー管理データベースと、
配信するデジタルデータの利用条件や格納場所の情報を記録するデジタルデータ管理データベースと、
各ユーザーが取得しているデジタルデータの配信を受ける権利に関する情報を記録する取得済権利管理データベースと、
ユーザーが過去に配信を受けたデジタルデータに関する情報を記録する履歴データベースと、
各ユーザーが使用しているアダプタのアダプタIDを記録するアダプタ管理データベースと、
各ユーザーが使用している記録媒体の媒体IDを記録する記録媒体管理データベースと、
暗号化されたデジタルデータと、前記暗号化されたデジタルデータを復号する復号鍵を記録する配信デジタルデータ記録手段と、
前記配信デジタルデータ記録手段に記録された復号鍵を、前記媒体ID検出手段から送られてくる媒体IDを利用して暗号化する鍵暗号化手段と、
前記配信フロントエンドからの指示に基づいて、前記受信端末にたいし、前記配信デジタルデータ記録手段に記録された暗号化されたデジタルデータと、前記鍵暗号化手段によって暗号化された復号鍵とを送信するデジタルデータ配信手段と
を有することを特徴とし、
前記アダプタ内のセキュア通信手段と、前記配信サーバー内のセキュア通信手段は、互いに通信しあい、前記アダプタと前記配信サーバー間にセキュアな通信経路を構築することを特徴とし、
前記アダプタ内の各構成要素と、前記配信サーバー内の各構成要素との通信は、前記

構築されたセキュアな通信経路を使用して行われることを特徴とし、
前記配信フロントエンドは、
前記アダプタ I D 検出手段から送信されてくるアダプタ I D を利用して、ユーザーの
認証を行い、
前記認証したユーザーからの、デジタルデータ配信要求に対して、前記取得済権利管
理データベースと、前記履歴データベースと、前記デジタルデータ管理データベ
ースと、前記記録媒体管理データベースの情報を参照して、前記配信要求されたデジタル
データが配信可か否かを判定し、処理を行う
ことを特徴とする
デジタルデータ配信システム。

2. デジタルデータを配信する配信サーバーと、
前記配信サーバーから配信されるデジタルデータを受信する受信端末と、
前記受信端末が受信したデジタルデータの書き込み先となる記録媒体と、
前記受信端末が受信したデジタルデータを前記記録媒体へ書き込むアダプタと
によって構成されるデジタルデータ配信システムであって、
前記受信端末は、
前記配信サーバーにアクセスするための通信手段と、
前記配信サーバーから送られてくる情報を閲覧しそれに応答するためのブラウズ手段
と、
前記アダプタとの接続を制御するアダプタ接続制御手段と
を有することを特徴とし、
前記記録媒体は、
改竄不可能な、その記録媒体を一意に識別することのできる固有の情報である媒体 I
D を有することを特徴とし、
前記アダプタは、
セキュア通信手段と、

そのアダプタを一意に識別することのできるアダプタ I D と、
前記アダプタ I D を抽出し、前記配信サーバーへ送信するアダプタ I D 検出手段と、
前記記録媒体から、前記媒体 I D を抽出し、前記配信サーバーへ送信する媒体 I D 検出手段と、
鍵暗号化手段と、
前記記録媒体にたいしてデータの読み書きを行う記録媒体アクセス手段と、
前記記録媒体アクセス手段による前記記録媒体への読み書きを制御する媒体アクセス処理制御手段と
を有することを特徴とし、
前記配信サーバーは、
セキュア通信手段と、
情報やデジタルデータを前記受信端末に送受信するための送受信手段と、
ユーザーへ送信する情報の生成およびユーザーからのアクセスを処理する配信フロントエンドと、
ユーザー I D と関連するユーザーのアカウント情報を記録するユーザー管理データベースと、
配信するデジタルデータの利用条件や格納場所の情報を記録するデジタルデータ管理データベースと、
各ユーザーが取得しているデジタルデータの配信を受ける権利に関する情報を記録する取得済権利管理データベースと、
ユーザーが過去に配信を受けたデジタルデータに関する情報を記録する履歴データベースと、
各ユーザーが使用しているアダプタのアダプタ I D を記録するアダプタ管理データベースと、
各ユーザーが使用している記録媒体の媒体 I D を記録する記録媒体管理データベースと、
暗号化されたデジタルデータと、前記暗号化されたデジタルデータを復号する復号鍵

を記録する配信デジタルデータ記録手段と、
前記配信フロントエンドからの指示に基づいて、前記受信端末にたいし、前記配信デジタルデータ記録手段に記録された暗号化され信デジタルデータと復号鍵とを送信するデジタルデータ配信手段と
を有することを特徴とし、
前記鍵暗号化手段は、前記デジタルデータ配信手段によって配信されてくる復号鍵を、前記媒体 I D 検出手段が検出した媒体 I D を利用して暗号化し、前記記録媒体アクセス制御手段は、前記記録媒体アクセス手段を制御して、前記鍵暗号化手段が暗号化した復号鍵を、前記記録媒体へ書き込むことを特徴とし、
前記アダプタ内のセキュア通信手段と、前記配信サーバー内のセキュア通信手段は、互いに通信しあい、前記アダプタと前記配信サーバー間にセキュアな通信経路を構築することを特徴とし、
前記アダプタ内の各構成要素と、前記配信サーバー内の各構成要素との通信は、前記構築されたセキュアな通信経路を使用して行われることを特徴とし、
前記配信フロントエンドは、
前記アダプタ I D 検出手段から送信されてくるアダプタ I D を利用して、ユーザーの認証を行い、
前記認証したユーザーからの、デジタルデータ配信要求に対して、前記取得済権利管理データベースと、前記履歴データベースと、前記デジタルデータ管理データベースと、前記記録媒体管理データベースの情報を参照して、前記配信要求されたデジタルデータが配信可か否かを判定し、処理を行う
ことを特徴とする
デジタルデータ配信システム。

3. デジタルデータを配信する配信サーバーと、
前記配信サーバーから配信されるデジタルデータを受信する受信端末と、
前記受信端末が受信したデジタルデータの書き込み先となる記録媒体と、

前記受信端末が受信したデジタルデータを前記記録媒体へ書き込むアダプタと
によって構成されるデジタルデータ配信システムであって、
前記受信端末は、
前記配信サーバーにアクセスするための通信手段と、
前記配信サーバーから送られてくる情報を閲覧しそれに応答するためのブラウザ手段
と、
前記アダプタとの接続を制御するアダプタ接続制御手段と
を有することを特徴とし、
前記記録媒体は、
改竄不可能な、その記録媒体を一意に識別することのできる固有の情報である媒体 I
Dを有することを特徴とし、
前記アダプタは、
セキュア通信手段と、
そのアダプタを一意に識別することのできるアダプタ I Dと、
前記アダプタ I Dを抽出し、前記配信サーバーへ送信するアダプタ I D検出手段と、
前記記録媒体から、前記媒体 I Dを抽出し、前記配信サーバーへ送信する媒体 I D検
出手段と、
暗号変換手段と、
鍵暗号化手段と、
前記記録媒体にたいしてデータの読み書きを行う記録媒体アクセス手段と、
前記記録媒体アクセス手段による前記記録媒体への読み書きを制御する媒体アクセス
処理制御手段と
を有することを特徴とし、
前記配信サーバーは、
セキュア通信手段と、
情報やデジタルデータを前記受信端末に送受信するための送受信手段と、
ユーザーへ送信する情報の生成およびユーザーからのアクセスを処理する配信フロン

トエンドと、

ユーザー I D と関連するユーザーのアカウント情報を記録するユーザー管理データベースと、

配信するデジタルデータの利用条件や格納場所の情報を記録するデジタルデータ管理データベースと、

各ユーザーが取得しているデジタルデータの配信を受ける権利に関する情報を記録する取得済権利管理データベースと、

ユーザーが過去に配信を受けたデジタルデータに関する情報を記録する履歴データベースと、

各ユーザーが使用しているアダプタのアダプタ I D を記録するアダプタ管理データベースと、

各ユーザーが使用している記録媒体の媒体 I D を記録する記録媒体管理データベースと、

第一の暗号化方式で暗号化されたデジタルデータと、前記第一の暗号化方式で暗号化されたデジタルデータを復号する復号鍵を記録する配信デジタルデータ記録手段と、前記配信フロントエンドからの指示に基づいて、前記受信端末にたいし、前記配信デジタルデータ記録手段に記録された第一の暗号化方式で暗号化されたデジタルデータと復号鍵とを送信するデジタルデータ配信手段と

を有することを特徴とし、

前記暗号変換手段は、前記デジタルデータ配信手段によって配信されてくる第一の暗号化方式で暗号化されたデジタルデータを、前記デジタルデータ配信手段によって配信されてくる復号鍵を使用して復号化し、復号化したデジタルデータを、第二の暗号化方式によって暗号化し、

前記鍵暗号化手段は、前記暗号変換手段がデジタルデータを第二の暗号化方式によって暗号化する際に使用した鍵を、前記媒体 I D 検出手段が検出した媒体 I D を利用して暗号化し、

前記記録媒体アクセス制御手段は、前記記録媒体アクセス手段を制御して、前記鍵暗

号化手段が暗号化した鍵を、前記記録媒体へ書き込むことを特徴とし、
 前記アダプタ内のセキュア通信手段と、前記配信サーバー内のセキュア通信手段は、
 互いに通信しあい、前記アダプタと前記配信サーバー間にセキュアな通信経路を構築
 することを特徴とし、
 前記アダプタ内の各構成要素と、前記配信サーバー内の各構成要素との通信は、前記
 構築されたセキュアな通信経路を使用して行われることを特徴とし、
 前記配信フロントエンドは、
 前記アダプタ I D 検出手段から送信されてくるアダプタ I D を利用して、ユーザーの
 認証を行い、
 前記認証したユーザーからの、デジタルデータ配信要求に対して、前記取得済権利管
 理データベースと、前記履歴データベースと、前記デジタルデータ管理データベー
 スと、前記記録媒体管理データベースの情報を参照して、前記配信要求されたデジタル
 データが配信可か否かを判定し、処理を行う
 ことを特徴とする
 デジタルデータ配信システム。

4. デジタルデータの配信を制御するデジタルデータ配信制御方法であって、
 請求項 1 ～ 3 何れかに記載のデジタルデータ配信システムにおいて、
 前記、配信フロントエンドが、
 前記アダプタ I D 検出手段から送信されてくるアダプタ I D を利用して、ユーザーの
 認証を行い、
 前記認証したユーザーからの、デジタルデータ配信要求に対して、前記取得済権利管
 理データベースと、前記履歴データベースと、前記デジタルデータ管理データベー
 スと、前記記録媒体管理データベースの情報を参照して、前記配信要求されたデジタル
 データが配信可か否かを判定し、処理を行うことを特徴とするデジタルデータ配信制
 御方法。

5. 請求項1～3何れかに記載のデジタルデータ配信システムであって、
前記アダプタは、前記アダプタ内のセキュア通信手段をアップデートするセキュア通信手段アップデート手段を有し、
前記配信サーバーは、
前記配信サーバー内のセキュア通信手段をアップデートするセキュア通信手段アップデート手段と、
必要に応じて、前記アダプタ内のセキュア通信手段アップデート手段と前記配信サーバー内のセキュア通信手段アップデート手段に、セキュア通信手段のアップデートを行うよう指示するセキュア通信手段アップデート指示手段と
を有することを特徴とするデジタルデータ配信システム